National Oceanic and Atmospheric Administration (NOAA)

National Environmental Satellite, Data and Information Service (NESDIS)

NESDIS E-Commerce System (NeS)

NeS Privacy Impact Assessment Statement

Prepared by: Duane Dunston, NCDC Information System Security Officer

Reviewed by: NESDIS E-Commerce System, Sarah Brabson, NOAA OCIO

NESDIS E-Commerce System (NeS)

Unique Project Identifier: 006-48-00-00-01-3209-00-109-023

Project Description

The National Environmental Satellite, Data and Information Service (NESDIS) E-Commerce System (NeS) is a system that handles customer order payment processing for orders both online (via the Online Store: http://www.ncdc.noaa.gov/oa/nolos/oluser.html) and offline (via direct interaction between customers and internal customer service representatives). NeS handles the product inventory, customer tracking for billing and shipping, accounting/fiscal processing, and reporting for the three NOAA National Data Centers:

1) National Climatic Data Center (NCDC): NCDC is the world's largest active archive of weather data.

2) National Geophysical Data Center (NGDC): NGDC provides stewardship, products, and services for geophysical data describing the solid earth, marine, and solar-terrestrial environment, as well as earth observations from space.

3) National Oceanographic Data Center (NODC): NODC archives & provides public access to global oceanographic and coastal data, products, and information.

1. What information is to be collected (e.g., nature and source)?

The information collected from a customer when placing an order includes the customer's name, billing address, phone number, and credit card number and expiration date, or "open account" information by which NCDC can bill for its products and services. The customer may place an order and provide the information over the Internet using the NCDC Online Ordering System, by facsimile, by surface mail, or over the phone.

2. Why is the information being collected (e.g., to determine eligibility)?

The information collected is needed by NCDC, NGDC, and NODC customer service employees to fill, cancel, or void orders and issue refunds when necessary.

3. What is the intended use of the information (e.g., to verify existing data)?

The information collected is needed by NCDC, NGDC, and NODC customer service employees to fill, cancel, or void orders and issue refunds when necessary.

4. With whom the information will be shared (e.g., another agency for a specified programmatic purpose)?

Customer information is used solely for the processing of customer orders, and is shared only with employees that need to know the information, namely customer service employees for NCDC, NGDC, and NODC. The information is never shared with third parties. Only pay.gov receives the individual customer's information via a Secure Socket Layer (SSL) connection, in order to charge for the order. SSL is a secure technology used to encrypt information from an individual's computer to a Web site when performing transactions over the Internet. A Web address that starts with *https://* indicates that an SSL connection is being used.

Under the provisions of the Privacy Act, individual customer information (name of individual, address, phone number, and credit card or other account information) is exempt from release in response to a Freedom of Information Act (FOIA) request, should one be received.

In the case of a FOIA request for information about orders from a business, only the business name, address, and phone number would be released. Account information and the name of the contact at the business are not provided.

5. What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

This statement appears at the bottom of each Web page:

"By sending us an electronic mail message, you may be sending us personal information (e.g., name, address, E-mail address). We may store the name and address of the requester in order to respond to the request or to otherwise resolve the subject matter of your E-mail. If you order weather data, we will enter the information you submit into our electronic database. This information will be used to fill your request and ship your data. In limited circumstances, including the Freedom of Information Act (FOIA), we may be required by law to disclose information you submit.

"We recommend that you do not use E-mail to submit credit card information to NCDC. Visit NCDC Security Issues to learn more about credit card security on our website.

"This privacy policy has been developed to comply with the requirement in Section 208 of the E-Government Act of 2002 (44 U.S.C. 36) and the Department of Commerce IT Privacy Policy."

Providing this information does not constitute a collection of information within the meaning of the Paperwork Reduction Act (PRA), and approval by the Office of Management and Budget (OMB) is not required.

6. How will the information be secured (e.g., administrative and technological controls)?

Operational Controls:

The NCDC data center where the servers are located is a facility staffed 24 hours a day, seven days a week with uniformed security guards. The computer room has a keycode entry system and is also staffed with computer operators 24 hours a day, seven days a week. Visitors and maintenance contractors must sign in at the guard desk, sign in upon entering and leaving the computer room, and be escorted at all times within the computer room. Data backup is performed daily, and the backup data is stored in a secure offsite location that only a limited number of people are allowed to enter. The backup facility also has a keycode entry.

Management Controls:

All employees and contractors undergo a national agency check with inquiries (NACI) security check when employed or contracted. This involves a check of federal and local law enforcement records to ensure the trustworthiness of the employee. Every three years, the IT system undergoes a thorough Certification and Accreditation (C&A) process that is performed by a contractor company. The C&A process ensures that the security plan and operational, management, and technical controls meet Department of Commerce (DOC) guidelines for continued operation. All security controls are reviewed and approved by the system and database administrators, developers, and managers prior to implementation. System security checks have to be performed regularly and reported to NESDIS Headquarters on a periodic schedule.

Technical Controls:

NCDC employs host-based and network Intrusion Detection Systems to help ensure that the systems containing customer information are not accessed by unauthorized users. Customer information is encrypted except when it is needed and being used by a customer service employee, who accesses the information using an encrypted connection. Specific IP addresses from NODC and NGDC are allowed access to the customer database at NCDC via the encrypted web interface.

Customer service employees must be assigned and enter a user ID and password to access customer information. Remote administration of the database and servers is performed over encrypted channels, and only specially approved users that need access to the servers are allowed to log in. Developers for NeS use test systems that do not contain customer information. Backups are performed on a daily basis and the customer information is kept encrypted on all backups.

7. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

A system of records notice for publication in the *Federal Register* has been drafted and is under review by the NOAA Privacy Act Officer. This notice will contain basically the same information as this Privacy Impact Assessment.